Testimony Before
The State of Michigan
Senate Banking and Financial Institutions Committee
On March 30, 2007

Alessandro P. DiNello
Executive Vice President
Flagstar Bank
Troy, Michigan

Chairman Richardville, and members of the committee. My name is Alessandro DiNello and I appreciate the opportunity to speak to you today. I am an Executive Vice President at Flagtar Bank, headquartered in Troy, Michigan. Flagstar operates 114 bank offices and 51 home loan centers throughout Michigan. Flagstar also provides full service banking services in Indiana and Georgia and provides lending services nationwide.

I have over 30 years experience in the banking industry, beginning as a bank examiner. I am currently director of retail banking at Flagstar and have responsibility for over 1000 team members. I also serve on the America's Community Bankers (ACB) Retail Banking, Operations, Security and Technology Committee. ACB is the leading trade association representing community banks nationwide.

I am here to speak to you about data security. Our Committee has been concerned with this issue for many years. Only recently though, has this topic gained much public attention; I'm sure you have all heard of the data security breach that occurred at TJX, where tens of millions of their customers may have experience a data security breach.

This issue is critical for all financial institutions. The TJX situation has clearly brought to light the risks that exist in today's electronic world. The growth of the Internet and electronic commerce has made compiling and selling sensitive personal information easier for a multitude of companies, and crooks, creating a need for comprehensive data security legislation.

Did you know that you can go on the Internet today and quite easily buy a fraudulent credit and/or debit card for $100 or less? I personally purchased

one off of a web site hosted somewhere in Russia. I contacted the person whose name was on the card, told them that that their information had been compromised and suggested that they contact their card provider.

We must focus on stopping the misuse of consumer information and create an incentive for companies to make securing customer data a priority. Financial institutions play no part in the cause of the breach, yet they are fully liable for fraudulent charges and for the majority of cost incurred to reissue compromised cards. Where is the fairness in this and why would a retailer spend money to prevent data breachs when they have no real responsibility for the consequences of their lack of data security?

Simply put, those that are responsible for a data breach must be responsible for the costs of protecting consumers from risks arising from the breach. Those responsible parties should bear the costs associated with notifying consumers of the breach, reissuing cards and fraudulent transactions resulting from the misuse of consumer information related to their breach.

Reissuing cards costs up to $10 to $20 each and the cost of fraudulent transactions can be thousands of dollars for each card which has been compromised. Why should banks bear the burden of these costs when they played no part in the cause of the problem?

This is a very big problem.

In a recent survey completed by the ACB, 70% of respondent banks said they had to reissue cards more than three times in the past 24 months; 39% reported having to reissue cards more five times. The math is easy; a bank reissuing 10,000 cards three times will experience a cost of close to half a million dollars; not including the losses from fraudulent transactions, which can be much, much more.

Clearly, retailers are failing to provide an appropriate level of data security, exposing consumers to serious risk of identity theft and imposing significant operational and reputational costs on banks.

For Flagstar specifically, just in connection with the TJX compromise, over 11,000 cards were compromised, including my wife and daughters, over 6,500 cards were reissued and losses from fraudulent transactions on over 100 cards total over $40k, and all these number continue to grow. This one

incident has cost our company well over $100k. The cost to all Michigan banks collectively is staggering, not to mention the inconvenience experienced by Michigan residents.

Your help is needed to put pressure on retailers to protect the information that they are entrusted with and to be financially responsible when they fail to do so.

I appreciate the opportunity to share these views with you and am happy to answer any questions you may have.